#12/a KW-S 10-23-02

Docket No.: 064808-0011

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of :

CHEN, JAY C. :

Serial No.: 09/456,794 : Group Art Unit: 2132

Filed: December 8, 1999 : Examiner: Meislahn, Douglas

For: **A CRYPTOGRAPHIC SYSTEM AND METHOD FOR ELECTRONIC TRANSACTIONS**

CERTIFICATE OF MAILING (37 C.F.R. § 1.8(a))

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail under 37 CFR 1.8(a) in an envelope addressed to Commissioner for Patents, Washington, DC 20231 on the date indicated below.

Date: 10/15/02 Marie W. Lau

AMENDMENT

Honorable Commissioner of
Patents and Trademarks
Washington, D. C. 20231

Attention: Douglas J. Meislahn

Commissioner:

In response to the Office action of July 2, 2002, please amend the above-identified application as follows:

In the Specification:

Please amend the specification as indicated below. A marked-up version of the changes made to the specification by the current amendment is attached hereto as Appendix A.

Please replace the entire text in the SUMMARY OF THE INVENTION section with the following replacement text:

In one aspect of the present invention, a method of conducting an electronic transaction using an electronic card having a public key of a service provider, includes initiating a transaction at a cardholder location by encrypting at least a portion of a message with the service provider's public key from the electronic card and sending the message to a service provider location, and completing the transaction between the cardholder and the service provider in response to the message.

In another aspect of the present invention, a method of conducting an electronic transaction using an electronic card having a public key of a service provider includes formatting a key exchange request message at a member, at least a portion of the key exchange request message being encrypted using the service provider's public key from the electronic card, sending the key exchange request message from the member to the service provider, generating a session key at the service provider in response to the key exchange request message, formatting a key exchange response message including the session key at the service provider, sending the key exchange response message from the service provider to the member, and using the session key to complete the transaction.

In yet another aspect of the present invention, a method of conducting an electronic transaction using an electronic card having a public key of a service provider includes generating a member challenge by the member, encrypting by the member the member challenge using the service provider's public key from the electronic card to generate a first cryptogram, formatting by the member a key exchange request message including the first cryptogram and a public key of the member, signing digitally by the member the key exchange request message, sending the digitally signed key exchange request message to the service provider, generating by the service provider a service provider challenge, generating by the service provider a session key, encrypting by the service provider the service provider challenge and the session key using the member's public key to generate a second cryptogram, formatting by the service provider a key exchange response message including the second cryptogram and a response to member challenge, signing digitally by the service provider the key exchange response message, sending the digitally signed key exchange response message to the member, encrypting by the member a member response for the service provider challenge using the session key to generate a third cryptogram, attaching the third cryptogram to a transaction

message going from the member to the service provider, signing digitally by the member the transaction message going from the member to the service provider, and sending the transaction message going from the member to the service provider to the service provider.

a' cont

In a further aspect of the present invention, a method of communication using an electronic card having a public key of a service provider includes formatting a first key exchange request message at a first member, the first key exchange request message having a public key of the first member, and at least a portion of the first key exchange request message being encrypted using the service provider's public key from the electronic card, sending the first key exchange request message from the first member to a second member, combining at a second member, a second member key exchange request message with the first member's key exchange request message and sending the combined key exchange request message, signed by the second member, to a service provider, formatting a key exchange response message at the service provider including a first session key for the first member, signing the response message, formatting a key exchange response message including a second session key for the second member, combining the key exchange response messages into a combined key exchange response message, signing the combined key exchange response message, and sending the combined key exchange response message to the second member, and separating at the second member, the key exchange response message for the second member from the key exchange response message for the first member, and forwarding the key exchange response message for the first member to the first member.

In yet a further aspect of the present invention, a method of communication using an electronic card having a public key of a service provider includes formatting a first key exchange request message at a first member, the first key exchange request message having a public key of the first member, and at least a portion of the first key exchange request message being encrypted using the service provider's public key from the electronic card, sending the first key exchange request message from the first member to at least one intermediate member coupled in series between the first member and the service provider, each of said at least one intermediate member being either a message router or a participating member, generating, if said at least one intermediate member

comprises at least one participating member, at each of the participating members a key exchange request, receiving at the service provider a combined key exchange request message from said at least one intermediate member, the combined key exchange request message comprising the first key exchange request message and the key exchange request message generated by each of the participating members, generating at the service provider a first session key for the first member and a participating session key for each of the participating members, formatting at the service provider a key exchange response message including each of the first and participating session keys, sending the key exchange response message from the service provider to said at least one intermediate member, separating by each participating member its respective participating session key from the key exchange response message, and sending the first session key from said at least one intermediate member to the first member.

In another aspect of the present invention, a method of communication using an electronic card having a public key of a service provider includes formatting a key exchange request message at each of a plurality of first members, the key exchange request message for one of the first members having a public key of said one of the first members, and at least a portion of the key exchange request message for said one of the first members being encrypted using the service provider's public key from the electronic card, sending from each of the first members its respective key exchange request message to a second member, the second member being either a message router or a participating member, generating, if the second member is a participating member, a second key exchange request message at the second member, combining at the second member the key exchange request message from each of the first members to form a combined key exchange request message, the combined key exchange request message further comprising the second key exchange request message if the second member is a participating member, receiving at the service provider the combined key exchange request message from the second member, generating at the service provider a first session key for each of the first members, and a second session key for the second member if the second member is a participating member, formatting at the service provider a key exchange response message including each of the first and second session keys, sending the key exchange response message from the service provider to the second